УДК 65.012.8 + 004

Володимир Володимирович ТУЛУПОВ,
кандидат технічних наук, доцент, доцент кафедри інформаційних технологій факультету № 4 Харківського національного університету внутрішніх справ

Валерій Миколайович ПЕРЕСІЧАНСЬКИЙ,
старший викладач кафедри інформаційних технологій факультету № 4 Харківського національного університету внутрішніх справ

ДЕЯКІ ОСОБЛИВОСТІ ПОШУКУ ТА ВСТАНОВЛЕННЯ ОСОБИ ПРИ РОЗСЛІДУВАННІ КІБЕРЗЛОЧИНІВ

У сучасній методиці боротьби з кіберзлочинністю одним із проблемних питань залишається встановлення та визначення місцезнаходження особи за її мережними ідентифікаторами, тобто за тими обліковими даними, яка особа залишила або надала інформацію про себе.

Одним із способів встановлення особи може виступати пошук інформації за певним ідентифікатором за допомогою різного роду сервісів та ресурсів [1, с. 256].

Знаючи наприклад IP-адресу комп'ютера або мережного обладнання особи та розуміючи правила надання доменних імен і закріплення їх за зонами, працівник правоохоронного органу здебільшого має змогу самостійно визначити фізичне місцезнаходження комп'ютера, за яким дана адреса закріплена.

Місцезнаходження програмно-технічних засобів у мережі Інтернет визначається також за IP - адресою, яка належить певному провайдеру і є взаємопов'язаною з номером телефону користувача послуг доступу до мережі (наприклад провайдера ВАТ «Укртелеком» за стандартом доступу ADSL) . Але цей спосіб пошуку та встановлення особи за допомогою офіційного запиту до власника ресурсу часто не дає бажаних результатів.

Тому, сьогодні існує декілька методів пасивного та активного збору інформації, програмних продуктів та утиліт за допомогою яких можна отримати відомості щодо власника домену (сайту), його IP-адреси та дізнатися, де розміщено сам сервер із сайтом (хостінг або Colocation) [2, с. 68].

Частіше використовують пасивний метод збору інформації який характерний тим, що його етапи неможливо виявити, тому що на практиці вони не викликають ніяких підозр, при

цьому фактично неможливо визначення вузла, з якого проводиться пасивний збір інформації.

За допомогою пасивного методу збору інформації в більшості випадків можна скласти приблизну карту вузлів зовнішнього периметра з припущеннями про їх роль, зібрати додаткову інформацію про організацію, контактну інформацію про особу та багато іншої корисної інформації. Одним із програмних продуктів, що допомагає при визначенні інформації різного виду в мережі Інтернет, є програма IP-Tools, що містить такі корисні утиліти як:

- Ping- Skanner – ping за діапазоном адрес або за списком адрес;
- Trace–показує маршрут, яким проходять IP-пакети між комп'ютерами;
- Whois–одержання реєстраційної інформації про домени з офіційних Whois серверів;
- Finger –одержання інформації про користувачів певного хоста;
- LookUp –визначає IP-адресу хоста або розташування самого сервера за іменем або навпаки.

Також у мережі Інтернет існують інші безкоштовні сервіси, за допомогою яких можна отримати ту чи іншу інформацію щодо ресурсів мережі (сайтів) (наприклад, SmartWhois, Mod IP, City тощо). За допомогою вказаних сервісів отримують інформацію про:

- належність конкретної IP-адреси до сегмента Інтернет певної країни, провайдера, хост-провайдера, їх контакти;
- IP-адресу певного сайту (ресурсу);
- реєстратора доменного імені певного сайту;
- технічну площадку (фізичне розташування) проксісервера;
- історію сайту, ресурс, який ним використовується, розрахунок трафіку, посилання на сайт тощо [2, с. 69].

Також слід використовувати сайти та програмні продукти які теж корисні при проведенні певного збору інформації наприклад:

- www.kali.org - Kali Linux продукт для пентесту тощо;
- www.edge-security.com/metagoofil.php - інструмент для збору інформації з документів які знаходяться в публічному доступі (Metagoofil використовує Google);
- www.archive.org - містить архів веб-сайтів;
- www.domaintools.com - розвідка доменних імен;

- www.alexa.com - база даних інформації про веб-сайти;
- www.serversniff.net - безкоштовні онлайн утиліти;
- www.centralops.net - безкоштовні онлайн утиліти;
- www.pipl.com - пошук людей;
- www.yoname.com - пошук людей в соціальних мережах і блогах;
- www.tineye.com - можна використовувати для визначення звідки зображення, чи є модифіковані версії;
- www.2ip.com.ua - безкоштовні онлайн утиліти.

Список використаних джерел:

1. Манжай О. В., Осятинська І. А. Встановлення та визначення місцезнаходження особи за її мережними ідентифікаторами // Актуальні питання розслідування кіберзлочинів : матеріали Міжнар. наук.-практ. конф., м. Харків, 10 груд. 2013 р. / МВС України, Харк. нац. ун-т внутр. справ. Х.: ХНУВС, 2013. С. 256.
2. Протидія кіберзлочинам: кримінально-правові та криміналістичні аспекти: посібник / [Р. І. Благута, О. В. Захарова, О. І. Зачек, М. Ю. Літвінов, Т. І. Созанський, І. А. Федчак]. Київ, 2012.

Одержано 17.10.2017